Ilari Karila

ACTIVE DIRECTORY JA IDENTITEETTIEN LAAJENTAMINEN PILVIPALVELUIHIN

Tietojenkäsittelyn koulutusohjelma

2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ACTIVE DIRECTORY JA IDENTITEETTIEN LAAJENTAMINEN PILVIPALVELUIHIN

Karila, Ilari
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2016
Ohjaaja: Grönholm, Jukka
Sivumäärä: 32
Liitteitä: 0

Asiasanat: Active Directory, Azure, käyttäjähallinta, BYOD

Tämän opinnäytetyön tavoitteena oli tutkia Active Directoryssa olevia käyttäjiä, niiden luontia ja hallinnointia sekä laajentamista pilvipalveluihin. Työ kirjoitettiin suoraan Satakunnan ammattikorkeakoululle.

Työstä selviää, miten Active Directory luo käyttäjän, antaa sille käyttöoikeudet resursseihin ja miten hyödynnetään sisäänrakennettuja käyttäjätilejä. Työssä myös tutkittiin käyttäjätilien toimivuutta pilvipalveluissa kuten Azure Active Directoryssa.

Työssä aineiston pohjana on käytetty julkisia www-sivuja, Active Directoryyn liittyvää peruskirjallisuutta sekä asiantuntijoiden kirjoittamia Microsoftin julkaisuja.

ACTIVE DIRECTORY AND EXPANDING IDENTITIES TO CLOUD SERVICES

Karila, Ilari
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
April 2016
Supervisor: Grönholm, Jukka
Number of pages: 32
Appendices: 0

Keywords: Active Directory, Azure, user management, BYOD

The purpose of this thesis was to examine the users of Active Directory, their creation and management, as well as the expansion of users to cloud services. Thesis was written directly to the Satakunta University of Applied Sciences.

This thesis shows how to create an Active Directory user, giving it access to resources, and how to use built-in user accounts. The thesis also examined the functioning of the user accounts in the cloud services like Azure Active Directory.

This thesis used materials found on the Internet, Active Directory-based literature, and Microsoft's publications.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön aiheena on Active Directory. Active Directory itsessään on niin iso kokonaisuus, että sen tarkasteluun tarvitsisi paljon laajemman työn. Siksi itse perehdyin tässä työssä vain käyttäjätilien hallintaan. Heti SAMKiin tullessa tiesin, että järjestelmähallinta tulee olemaan minun osaamisalueeni. Lisää kiinnostusta herättivät palvelinkurssit. Active Directorya käytiin läpi vain muutaman opintojakson verran. Muutaman kurssin jälkeen halusin saada lisätietoa Active Directorysta. Tähän väliin astui työharjoittelu, joka sisälsi suureksi osaksi AD:n käyttämistä ja ymmärrystä. Työtehtäviin kuului olla AD-operaattori. Hallinnoin kaikkia työntekijöitä ja heidän käyttäjätilejään AD:n kautta. Kyseisen työn ansiosta sain paljon konkreettista käsitystä, että miten Active Directory toimii työtehtävissä. Active Directory on olemassa useimmissa työpaikoissa ja uskon, että tuleva työtehtävä tulee sisältämään Active Directoryn hallintaa.

Työ käsittelee alussa yleisesti Active Directorya. Mikä kaikki AD:ssa vaikuttaa käyttäjiin ja mistä AD koostuu. Koska työ pitää enimmäkseen tietoa käyttäjistä, tutkitaan seuraavana käyttäjäprofiilia. Millaisia profiileja voidaan luoda ja miten ne toimivat tietyissä ympäristöissä. Kun profiilit ovat selvitettyinä, tutkitaan käyttäjätilejä ja niiden erilaisia mahdollisuuksia toimia Active Directory ympäristössä. Kerrotaan yleisesti Administrator- ja Guest-tilien toiminnallisuudesta. Lopuksi tehdään vielä pieni katsaus AD:n Active Directory Users and Computers –hallintakonsoliin. Tämän jälkeen laajennetaan käyttäjiä pilvipalveluihin ja esitellään erilaisia pilvessä toimivia sovelluksia.

2 ACTIVE DIRECTORY

2.1 Yleistä

Active Directory (AD) on Microsoftin kehittelemä tuote. Active Directory perustuu useisiin standardeihin, esimerkiksi LDAP, DNS, KERBEROS, SNTP, DHCP, jne. Ensimmäisiä versioita Active Directorysta on esitelty vuonna 1996, mutta varsinaiset julkaistut versiot ovat tulleet vasta vuonna 1999–2000 Windows 2000-käyttöjärjestelmän mukana. Nykyisin Active Directory toimii Windows-palvelinten ja –verkkojen kanssa tarjoten liittymärajapintoja myös muihin samankaltaisiin palveluihin. (Teleware Oy, haettu 25.2.2015.)

Active Directory on yrityksen sisäisen toimialueen käyttäjätietokanta ja hakemistopalvelu. Sen tarkoituksena on varastoida organisaation henkilökunnan käyttäjätunnukset ja muut perustiedot. Active Directory rakentuu hierarkkisen tietokannan ylläpitämiseen, jonka avulla järjestelmän ylläpitäjät voivat hallita ja muokata tietoja. Tällaisia tietoja voivat olla esimerkiksi käyttäjätiedot ja –oikeudet, sovellusohjelmien jaot, ohjelma- ja järjestelmäasetukset sekä resurssien haku. Active Directoryyn ottavat yhteyttä ne palvelut, jotka haluavat varmistaa käyttöoikeudet henkilöltä. (Tolvanen 2011, haettu 25.2.2015.)

2.2 Toimialue

Toimialue käsittää ryhmän tietokoneita ja laitteita verkossa, jota hallitaan yksikkönä ja jolla on omat säännöt ja käytännöt. Internetin sisällä, toimialueet on määritelty IP-osoitteen mukaan. Laitteet toimialueen sisällä, jotka jakavat osan IP-osoitteesta, sanotaan kuuluvan samaan toimialueeseen. (Posey 2006, haettu 26.4.2016.)

Active Directory käsittelee tietojaan objekteina. Kyseiset objektit talletetaan järjestelmän hierarkkisesti ylläpidettyyn tietokantaan. Objektit jaotellaan kolmeen erilaiseen kategoriaan: resurssit, palvelut ja henkilöt. Active Directory järjestää kyseisten tietojen tallentamisen, järjestelemisen, käyttöoikeudet ja tietoturvan. (Microsoft 2016, haettu 21.4.2016.)

Active Directory -hakemistoon talletettu objekti oletettavasti sisältää yksilöllistä tietoa; se antaa kuvaa yksittäisestä käyttäjästä, käyttäjäryhmästä, työasemasta, palvelimesta, tulostimesta, sovelluksesta, jne. Kaikki objektit nimetään yksilöllisesti ja jokaisella objektilla on tyypillisesti yksi tai useampi attribuutti, johon tiedot objektista tallennetaan. (Microsoft 2016, haettu 21.4.2016.)

Kaikki objektit tietokannan sisällä tunnetaan nimellä toimialue. Tiedot objekteista tallennetaan toimialueeseen, johon objekti kuuluu. Puu pitää sisällään yhden tai useamman toimialueen vierekkäisistä nimiavaruuksista. Metsä on kokoelma puista ja esittää kokonaisuutta, jossa sisältyvät kaikki käyttäjät, tietokoneet, ryhmät ja muut objektit. Metsä toimii turvallisuuden rajana Active Directorylle. (Hephaestus Books 2.)

Metsille voidaan asettaa luottamussuhde. Se käsittää kaksi Active Directoryn metsää yhden organisaation sisällä. Yksi metsä sijaitsee organisaation ulkoverkossa. Toinen metsä sisäverkossa. Yksisuuntainen luottamus tehdään niin, että metsä ulkoverkossa luottaa sisäverkon metsään. Federaatio palvelimet ovat käytössä molemmissa verkoissa. Luottamus on asetettu niin, että käyttäjätilejä sisäisestä metsästä voidaan käyttää www-pohjaisesta sovelluksesta ulkoverkosta käsin. Tämä toimii sisäverkosta käsin kuin myös Internetistä. (Microsoft 2014, haettu 15.4.2016)

3 KÄYTTÄJÄPROFIILIT

3.1 Yleistä

Käyttäjäprofiilit sisältävät kaikki ympäristöasetukset käyttäjästä. Kun käyttäjä omalla profiilillaan kirjautuu sisään, järjestelmä tunnistaa työpöydän, ohjauspaneelin asetukset, valikkokomennot, sovellukset sekä muutaman muun asetuksen. Käyttäjäprofiili tuo myös työpöydän yhdenmukaisuuden, koska järjestelmä muistaa työpöydän edelliseltä kirjautumiselta. (Kivimäki 2005, 420.)

Käyttäjäprofiili voi myös olla useiden ihmisten käytössä ns. yleisprofiilina. Yleisprofiili voi aiheuttaa organisaatiolle tietoturvariskin. Koska yleisprofiiliin tallentuvat kaikki ympäristöasetukset ja ryhmäkäytännöt, sitä on vaikeampi pitää hallinnassa. Yleisprofiilin salasana on kaikille sama, jonka murrosta voi aiheutua mittavat sanktiot. Jokainen kirjautuminen järjestelmään luo paikallisen kopion käyttäjän profiilista. Tämä tapahtuu jokaisen eri kirjautuvan profiilin kohdalla. Profiilit tallentuvat kiintolevylle, joka sisältää useamman käyttäjän profiilin. Vastaavasti käyttäjäprofiilit voivat olla tallennettuna useampaan koneeseen. Toinen tietokone ei voi ottaa käyttöönsä paikallisesti tallennettua profiilia, joka on toisessa tietokoneessa. Nämä ovat paikallisia profiileja (local user profile). Jos käyttäjä kirjautuu vuorotellen moneen eri tietokoneeseen, voi hänellä olla erilaisia profiileja. Käyttäjän asetukset ovat erilaiset aina kussakin järjestelmässä. (Kivimäki 2005, 420-421.)

Käyttäjälle voidaan luoda juokseva profiili, joka tulee palvelimelta suoraan (Roaming Profile). Tällainen profiili on käytettävissä kaikissa järjestelmissä, joista käyttäjä kirjautuu toimialueelle. Palvelinpohjaisessa kirjautumisessa käyttäjät saavat saman profiilin käyttöönsä riippumatta siitä, mihin tietokoneeseen kirjautuvat. Kun käyttäjä kirjautuu järjestelmään, tämä luo paikallisen kopion profiilista. Tätä profiilia käytetään koko istunnon ajan. Kun käyttäjä kirjautuu ulos järjestelmästä, profiili ja siihen tehdyt muutokset kopioituvat paikalliseen työasemaan, josta siirtyvät palvelimelle. (Kivimäki 2005, 421.)

Järjestelmänvalvoja voi myös asettaa pakollisen profiilin (mandatory user profile). Käyttäjät, joille määrätään pakollinen profiili, voivat tehdä vain hetkellisiä muutoksia järjestelmään; nämä muutokset ovat voimassa vain kyseisen kirjautumisen ajan. Paikalliseen järjestelmään ei tallenneta mitään muutoksia, joten kun käyttäjä kirjautuu seuraavan kerran, käyttää järjestelmä alkuperäistä profiilia. Näin käyttäjät eivät pysty vahingoittamaan ympäristöään, eivätkä muutokset voi aiheuttaa ongelmia. (Kivimäki 2005, 420.)

3.2 Toimintaperiaate

Kun ensimmäisen kerran käyttäjä kirjautuu sisään, luodaan paikallinen profiili. Kun profiili on luotu, se tallennetaan kyseisen tietokoneen kiintolevylle. Käyttäjäprofiili saa aina käyttöönsä omat työpöytäasetukset ja yhteydet. Muilla käyttäjillä ei ole merkitystä. Järjestelmä voi myös luoda käyttäjän paikallisen Default User –kansion. Kansio tallentuu kohteeseen %systemdrive%\Documents and Settings\<kirjautumistunnus>. (Normaalisti C:\Users\%username%). On olemassa myös asetuksia, jotka luovat käyttäjäkansiot profiilikansioon %Systemroot%\Profiles, Documents and Settings –kansion sijaan. (Kivimäki 2005, 421.)

Käyttäjäprofiilikansio pitää sisällään useita käyttäjän tiedostoja ja kansioita.
Kansiot ovat seuraavat:

- Application data: sovelluskohtaiset tiedot, kuten tekstinkäsittelyohjelman muokattu sanasto
- Cookies: Internet Explorerin evästeet (keksit, taikapiparit, cookies)
- Desktop (Työpöytä): työpöydän pikakuvakkeet ja tiedostot
- Favorites: Internet Explorerin suosikit
- Local Settings: paikalliset sovellusasetukset ja muut tiedot, joita ei kopioida profiilin mukana (alikansiot: Application data, History, Temp, Temporary Internet Files)
- My Documents (Omat Tiedostot): paikka, johon tallennetaan henkilökohtaiset tiedostot. Oletusarvon mukaan myös File Open- ja Save As –komennot käyttävät My Documents –kansiota. Alikansiot: Omat kuvatiedostot (My Pictures) ja Omat musiikkitiedostot (My Music)
- Start Menu (Käynnistä-valikko): pikakuvakkeet sovelluksille
- Templates (Mallit): pikakuvakkeet mallitiedostoille.

(Kivimäki 2005, 422.)

4 KÄYTTÄJÄTILIEN HALLINTA

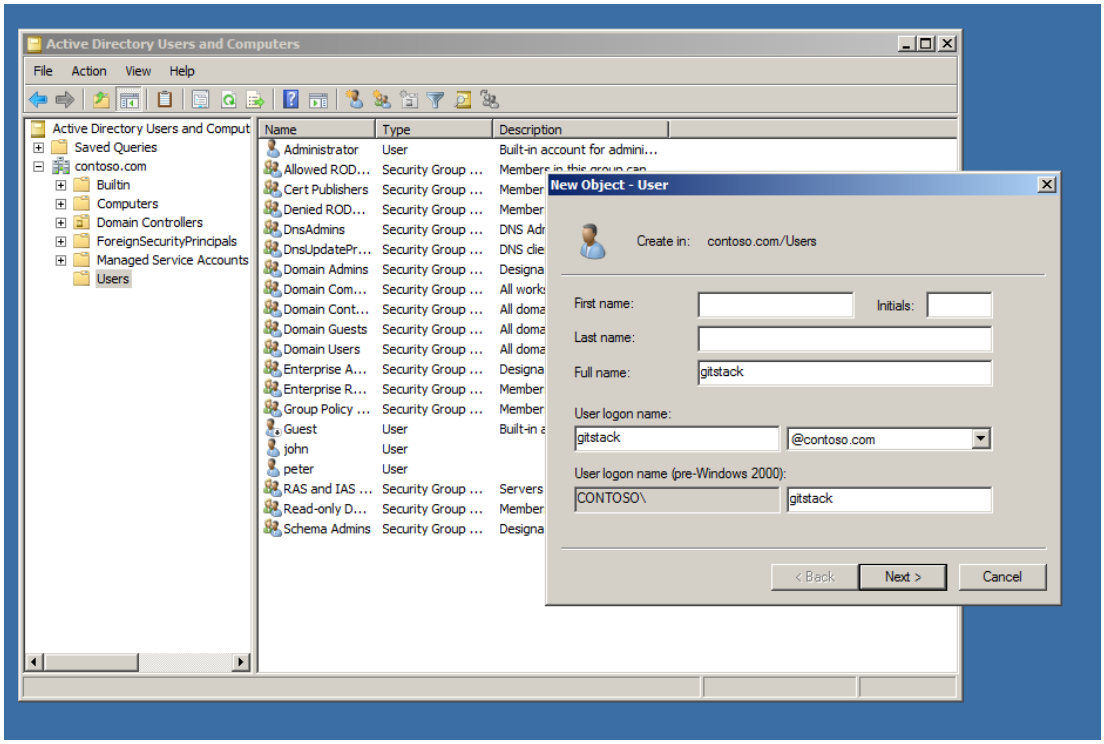
4.1 Yleistä

Käyttäjätilien hallinnalla usein tarkoitetaan tilien käyttäjäprofiilien ja asetusten muuttamista sekä kotikansioiden määrityksiä. Käyttäjätilien avulla kirjaudutaan sisään paikalliseen järjestelmään tai toimialueeseen. Active Directory voi myös määrittää erilaiset käyttöoikeudet toimialueen objekteihin sekä resursseihin (tulostimet, jaetut kansiot jne.) Käyttäjätilit ovat paikallisia tai toimialueen käyttäjätilejä. Usein paikallisesti kirjautuva käyttää paikallisia resursseja (Kivimäki 2005, 388). Järjestelmänvalvoja voi tarvita paikallisia tunnuksia silloin, kun toimialueen verkossa voi olla kirjautumisongelmia.

Käyttäjätili, joka kirjautuu toimialueelle, saa käyttöönsä toimialueen resurssit. Toimialue edellyttää Active Directoryn asentamista. On olemassa myös sisäänrakennettuja käyttäjä- ja ryhmätilejä: esimerkiksi järjestelmänvalvojan tilillä saadaan suoritettua järjestelmän hallinnan tehtäviä. Käyttäjätili tulee luoda jokaiselle, joka haluaa käyttää toimialueen resursseja. Jokainen uusi käyttäjätili saa tietyt oletusarvoiset ominaisuudet ja käyttöoikeudet. (Kivimäki 2004, 385; Kivimäki 2005, 388.)

Käyttäjiltä edellytetään todennusta eli autentikointia. Usein Active Directorystä käsin määritellään uudelle käyttäjälle esimääritelty salasana tai pakotettu salasanan vaihto ensimmäisen kirjautumisen yhteydessä. Todennuksella varmistetaan käyttäjän tai objektin identiteetti. Kun todennetaan objekti, sen tarkoituksena on varmistaa, että objekti todella on aito. Kun todennetaan käyttäjä, varmistetaan ettei kyseessä ole huijari. (Microsoft 2014, haettu 15.4.2016.)

Autentikoinnin kanssa toinen turvallisuusmenetelmä on autorisointi, eli valtuutus. Ero näiden kahden välillä on, että autentikointi osoittaa, että sinä olet kuka sanot olevasi. Autorisointi tarkistaa, että sinulla on riittävät valtuudet tehdä sitä mitä olet tekemässä. (Microsoft 2014, haettu 15.4.2016.)

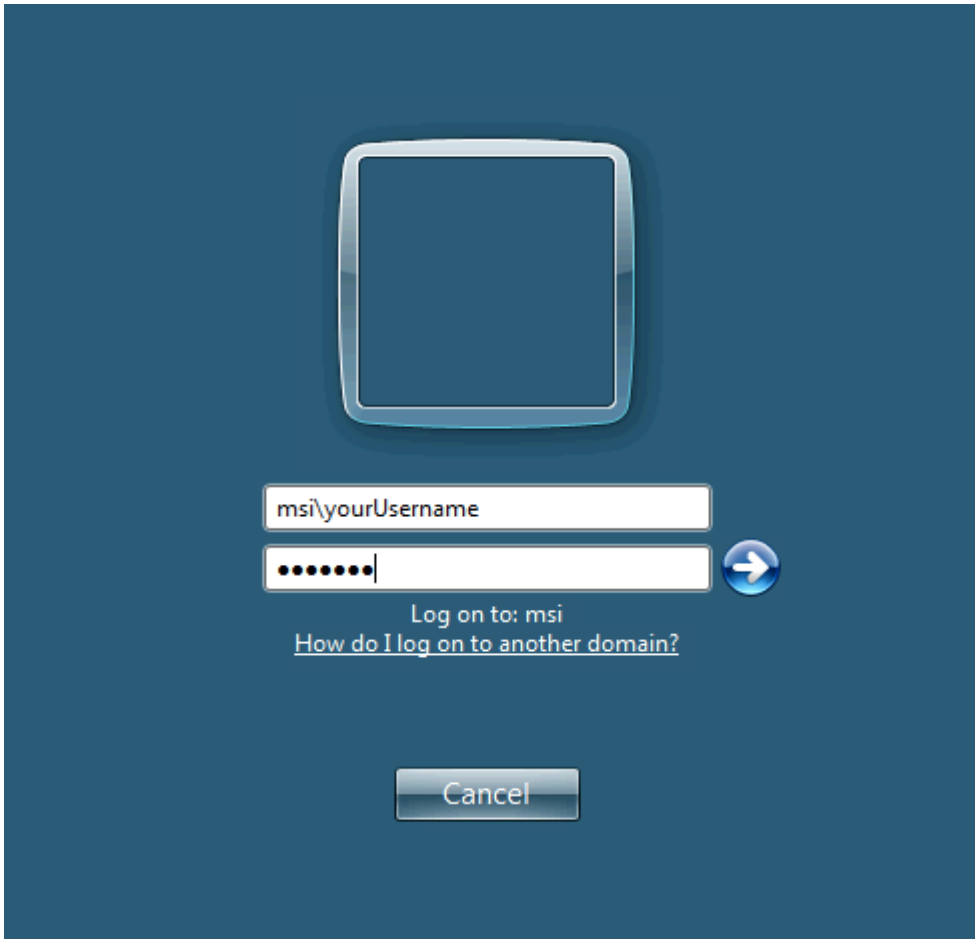


Kuva 1. Active Directory Users and Computers työkalu, jolla luodaan ja hallinnoidaan käyttäjiä ja käyttäjäryhmiä.

4.2 Paikallinen käyttäjätili

Paikalliset käyttäjätilit mahdollistavat istunnot siinä tietokoneessa, johon tili on luotu. Tällöin voidaan käyttää vain paikallisen tietokoneen resursseja. Paikalliset käyttäjätilit tallennetaan kyseisen järjestelmän paikalliseen suojaustietokantaan. (Kivimäki 2004, 386; Kivimäki 2005, 389.)

Käyttäjän kirjautuessa järjestelmään, tämä tarkistaa käyttäjän kirjautumistunnukset paikallisesta suojaustietokannasta. Järjestelmä jakaa käyttäjälle oikeuden kirjautua kyseiseen työasemaan. Kirjautumisen jälkeen käyttäjä saa järjestelmän resurssit käyttöönsä. Paikallista käyttäjätietokantaa ei pystytä poistamaan. Sitä ei myöskään voi kopioida. Siitä pystyy ottamaan varmistuksen käyttämällä varmistusohjelmaa. (Kivimäki 2004, 386; Kivimäki 2005, 389.)



Kuva 2. Kirjautumisikkuna.

Paikallisia käyttäjätilejä ei replikoida toimialueen ohjauspalvelimiin (domain controller). Toimialueen suojaustietokantaa käsittelevät vain domain controllerit. Toimialueelle voidaan lisätä erillispalvelin jäseneksi (member server). Tällöin toimialueen yleiset ryhmät liitetään paikallisiin ryhmiin (Domain Users – Users ja Domain Admins – Administrators). Tämä antaa toimialueella kirjautuneille käyttäjille oikeudet käyttää tai hallinnoida toimialueella olevaa jäsenpalvelinta. Jäsenpalvelimet kuitenkin käyttävät omaa paikallista käyttäjätietokantaansa. (Kivimäki 2004, 386; Kivimäki 2005, 389.)

Kun työasema otetaan mukaan toimialueelle, toimialueen yleiset ryhmät liitetään paikallisiin ryhmiin. Työasema käyttää edelleen paikallista käyttäjätietokantaansa. Toimialue ei tunnista paikalliseen työasemaan liitettyjä käyttäjätilejä. Paikallisille käyttäjätileille ei myöskään voi antaa toimialueelle kuuluvien resurssien käyttöoikeuksia. (Kivimäki 2004, 387; Kivimäki 2005, 389-390.)

Paikallinen käyttäjä voi hyödyntää resursseja toisesta tietokoneesta vain jos

- sama käyttäjätili ja salasana ovat voimassa toisessa tietokoneessa (Oppilas1:oppilas1)
- toisessa tietokoneessa on otettu käyttöön Vieras (Guest) –käyttäjätili
- kyseessä on resurssi, jonka anonyymi käyttö on sallittu
- paikallisesti kirjautunut käyttäjä tuntee käyttäjätilin sekä salasanan, jolla resurssin voi ottaa käyttöön.

(Kivimäki 2004, 387.)

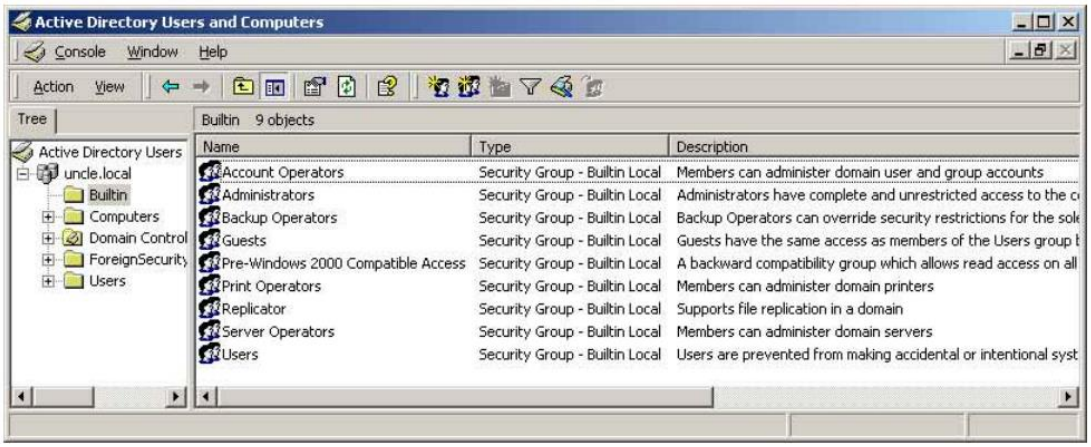
4.3 Toimialueen käyttäjätilit

Toimialuetason käyttäjätili pystyy kirjautumaan toimialueelle ja käyttämään sen resursseja. Sisäänkirjautuminen vaatii käyttäjänimen ja salasanan. Nämä tunnistetiedot (credentials) tunnistavat käyttäjän. Tämän jälkeen järjestelmä luo käyttäjälle saantitunnuksen (Access Token), joka sisältää käyttäjätilin suojausasetukset ja oikeudet. Saantitunnus on voimassa koko istunnon ajan. (Kivimäki 2004, 387-388; Kivimäki 2005, 391.)

Active Directory Users and Computers –hallintakonsolilla luodaan kaikki toimialueen käyttäjätilit. Active Directory Users and Computers –hallintakonsoli vaatii riittävät järjestelmänvalvojan oikeudet. Usein kyseessä on Domain Admins -ryhmä. Yleensä toimialuetason käyttäjätilit luodaan organisaatioyksikköön. Tämä yksikkö sijaitsee toimialueen ohjauspalvelimessa Active Directoryn hakemiston kopiossa (replika). Ohjauspalvelin replikoi käyttäjätilin muihin ohjauspalvelimiin. Kun replikointi on suoritettu, kaikki toimialueen ohjauspalvelimet pystyvät tunnistamaan käyttäjätilin. Toimialueen ja työasemien välillä voi toimia luottosuhde. Näistä koostuu luotettu toimialue (trusted domain). Tällöin käyttäjätili voi kirjautua luotetun toimialueen käyttäjätunnuksilla. (Kivimäki 2004, 388; Kivimäki 2005, 391-392.)

4.4 Oletuskäyttäjätilit ja –ryhmät

Windows käyttöjärjestelmä asentaa automaattisesti tietyt oletuskäyttäjät ja –ryhmät. Valmiit eli esimääritellyt (Predefined) käyttäjä- ja ryhmätilit ovat paikallisia siinä järjestelmässä, johon ne asennetaan. Esimäärätyille tileille on olemassa oma vastine Active Directoryssa. Kyseiset tilit ovat taas koko toimialueen laajuisia ja ovat täysin erillisiä järjestelmien paikallisista käyttäjätileistä. Sisäänrakennetuilla (Built-In) tileillä on usein erikoiskäyttötarkoitus. Sisäänrakennettuja tilejä asennetaan käyttöjärjestelmän, sovelluksen tai palvelun toimesta (esimerkiksi Active Directory). Yksi esimerkki tällaisesta tilistä on LocalSystem. Implisiittiset (Implicit) tilit ovat erikoisryhmiä. Ne ovat luotu implisiittisesti käyttäen verkon resursseja. Näitä tilejä kutsutaan myös erikoisidentiteeteiksi. (Kivimäki 2004, 392.)



Kuva 3. Builtin-kansio ja sisäänrakennetut ryhmätilit.

4.5 Esimääritellyt käyttäjätilit

Käyttöjärjestelmät sekä Active Directory luovat asennuksen yhteydessä valmiit käyttäjätilit. Näistä kaksi yleisintä ovat Administrator- ja Guest-tilit. Näitä tilejä ei pysty poistamaan käyttöjärjestelmästä. Oletuksena Administrator-tilin käyttöä ei pystytä estämään. Käyttäjätileistä voidaan muuttaa nimet. (Kivimäki 2004, 393; Kivimäki 2005, 393.)

Administrator-käyttäjätili on ensimmäinen tili, joka luodaan kun Active Directory on asennettu. Administrator-käyttäjätilillä suoritetaan kaikki toimialueen konfigurointitehtävät, kuten käyttäjätilien ja ryhmien luonti ja ylläpito, suojauskäytäntöjen hallinta sekä resurssien käyttöä koskevat käyttöoikeudet. Toimialueella Administrator-tilillä on toimialueelle pääsyoikeudet ja valtuudet. (Shinder, Shinder, Martin 2003, 102; Kivimäki 2004, 394; Kivimäki 2005, 393.)

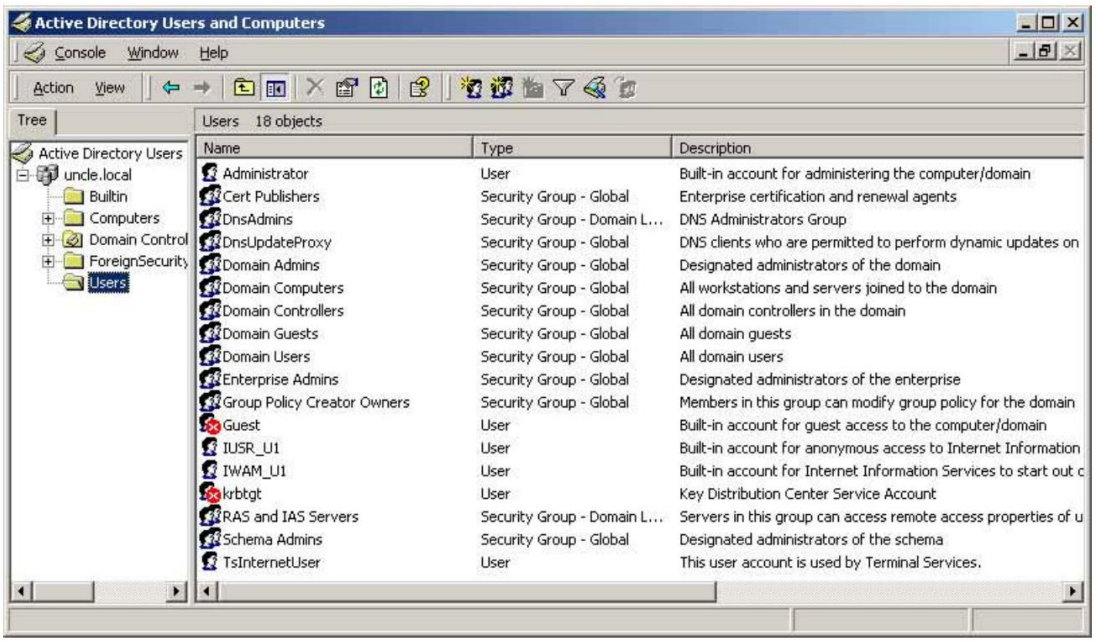
Administrator-ryhmään kuuluvia käyttäjätilejä ovat

- Domain Admins: toimialueen järjestelmänvalvojat
- Domain Users: toimialueen käyttäjät
- Enterprise Admins: yrityksen järjestelmänvalvojat
- Group Policy Creator Owners: ryhmäkäytäntöjen luojat/omistaja.

(Kivimäki 2005, 394.)

Enterprise Admins –ryhmän jäsenet saavat oikeudet hallinnoida koko toimialuepuu-ryhmää eli metsää. Tästä syystä metsän ensimmäisellä toimialueen Administrator-käyttäjätilillä on enemmän oikeuksia kuin muiden toimialueiden Administrator-käyttäjätileillä. (Kivimäki 2004, 394.)

Guest-tilillä on vähiten oikeuksia built-in tileistä. Guest-käyttäjätili antaa käyttäjälle oikeudet kirjautua verkkoon ja käyttää toimialueelle kuuluvia resursseja. Pääasiallisesti tili on tarkoitettu tilapäiseen käyttöön, esimerkkinä kirjautuminen vieraaseen tietokoneeseen, jossa henkilön on saatava tarvittavia resursseja käyttöönsä. Oletuksena Guest-käyttäjätili on poistettu käytöstä (Disabled). Guest-tilin salasana ei vanhene, eikä käyttäjä voi muuttaa sitä. Tilillä yleisesti pääsee vain suojausvaatimuksiltaan alhaisiin verkkoihin. Guest-tili on oletusarvoisesti Active Directoryn –toimialueilla Domain Guests- ja Guests –ryhmien jäsen. (Shinder ym. 2003, 103; Kivimäki 2005, 395.)



Kuva 4. Users-kansio ja esimääritellyt käyttäjä- ja ryhmätilit.

5 ACTIVE DIRECTORY USERS AND COMPUTERS

5.1 Yleistä

Active Directory Users and Computers (ADUC) on tullut Windows 2000 aikoihin. Se on työkalu, jota melkein jokainen järjestelmänvalvoja käyttää. AD:n hallintaohjelmana ADUC tarjoaa työkalut hallita käyttäjiä ja ryhmiä, sekä etsintä- ja lukutyökaluna hakemistoille ja ylläpitotehtäville. Eli sillä hallitaan toimialuetta. ADUC:n avulla voidaan tarkastella esimerkiksi ohjauspalvelinten roolit, toimialueen toimintatilat ja toimialueen objektit. ADUC:n käyttö vaatii riittävät oikeudet hallittaviin objekteihin. (Kivimäki 2004, 291; Desmond, Richards, Allen & Lowe-Norris 2013, 37-38.)

Käyttäjätili luodaan jokaiselle verkon resursseja käyttävälle. Graafisella ADUC- konsolilla (Kuva 1) voidaan saada uusi käyttäjätili muutamalla valinnalla. Tämän avulla voidaan luoda isoja määriä käyttäjätilejä. ADUC sisältää myös toiminnon (Copy Object – User), joka kopio valmiista käyttäjätilistä toisen. Kopioitu käyttäjätili saa useimmat ympäristöasetukset kopioitavalta tililtä. Usein käyttäjätili sisältää etunimi, sukunimi ja mahdollisen yksilöllisen käyttäjänimen. Käyttäjätilin luomisen aikana ei ole

pakko antaa tilille salasanaa. Tämä on riippuvainen organisaation salasanakäytännöistä. (Stanek 2003, 163; Kivimäki 2004, 466-467; Kivimäki 2005, 457-458.)

6 BYOD

6.1 Yleistä

Pilvipalvelut ovat kokoelma it-palveluita ja infrastruktuureita, jotka ovat käytettävissä verkossa. Vastakohtana olisi käyttää yrityksen palveluita paikallisesti rakennuksen sisällä, jossa palvelin sijaitsee. Pilvipalvelut tarjoavat samat palvelut verkon yli kuin sisäinen palvelin. Pilvipalvelun tarkoituksena on sallia käyttäjän pääsy yrityksen palveluihin kaikkialta. Yritys voi sallia kaikki toiminnot pilviin. (Carter 2012, haettu 12.4.2016)

Bring Your Own Device eli tuodaan oma laite töihin. Nykyaikana kasvava trendi on tuoda omia laitteita työpaikalle. Laitteita voivat olla esimerkiksi mobiililaitteet, kannettavat tietokoneet ja puhelimet. BYOD tuo yritykselle muutamia hyötyjä. Se ajaa kuluja käyttäjille, jotka ostavat omia laitteitaan. Työntekijät ovat myös tyytyväisempiä käyttäessään omia laitteita. Usein myös käyttäjien omat laitteet ovat markkinoiden uusimpia, joten työpaikka hyötyy niiden uusista ominaisuuksista ja tehoista. (Bradley 2011, haettu 12.4.2016)

BYOD tuo myös haittoja. Ensimmäinen suuri haitta on IT-tuen kontrolli laitteisiin. IT-tuki hallinnoi yrityksen omia laitteita ja määrittää niihin omat suojauskäytännöt. IT-tuki ei välttämättä kykene käskemään mitä heidän työntekijät tekevät omilla laitteillaan. BYOD laitteille joudutaan tekemään omat suojauskäytännöt ja säännöt. Niille joudutaan antamaan erilaisia pääsyoikeuksia järjestelmiin, jotka voivat olla vaarana saastua käyttäjän huolimattomuuden takia. Yritys joutuu myös tekemään erilaisia sääntöjä koskien sisäistä verkkoa ja miten se suhtautuu tuntemattomiin laitteisiin. (Bradley 2011, haettu 12.4.2016)

Pitää myös miettiä datan omistusta. Jos työntekijä lopettaa yrityksessä, tarvitsee yrityksen saada omat datansa takaisin työntekijältä. Yrityksellä tulisi olla sääntö, jota noudatetaan tilanteessa, missä pitää työpaikan tiedot saada työntekijän puhelimesta tai tietokoneesta. Tietyt yrityksen tiedot ovat salassa pidettäviä, vaikka ne olisi työntekijän omalla koneella. (Bradley 2011, haettu 12.4.2016)

Active Directory Federation Services on identiteettien silta AD metsän ja ulkoverkon palvelujen välillä. Windows Server 2012 R2 versiossa ADFS ja AD Domain Services on laajennettu niin, että ne ymmärtävät useimmat mobiililaitteet sekä niiden sisäänpääsy käytännöt. (Deuby 2013, haettu 20.4.2016)

6.2 Active Directory Workplace Join

BYOD ominaisuudet mahdollistaa käyttöön AD Workplace Join. Tämä muistuttaa hieman Windowsin tavallista toimialuetta, mutta on kevyempi. Kun mobiililaite rekisteröidään Workplace Joinin kanssa, AD luo laiteobjektin liitettynä AD käyttäjätunnukseen, joka omistaa laitteen. Käyttäjän puolella luodaan käyttäjä@laite sertifikaatti. Tämä asennetaan mobiililaitteeseen ja se on liitettynä laiteobjektiin AD:n sisällä. (Deuby 2013, haettu 20.4.2016)

Kun laite on tunnistettu luotettavaksi objektiksi, IT-tuki voi tämän jälkeen myöntää pääsyjä käyttäjä/laitteelle. Koska laite on tunnistettu luotettavaksi, sitä voidaan käyttää kertakirjautumiseen ilman että tarvitaan erikseen suojakortteja. (Deuby 2013, haettu 20.4.2016)

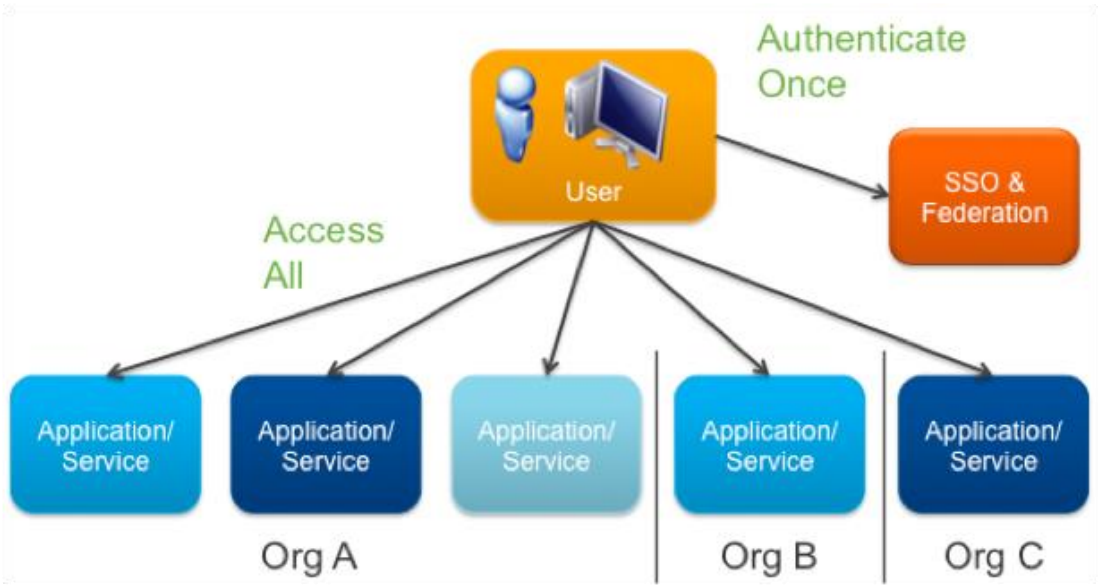
7 SINGLE SIGN-ON

7.1 Yleistä

Single sign-on (SSO) tarkoittaa kertakirjautumista. Sen ideana on hyödyntää käyttäjän autentikointia niin, että käyttäjä kirjautuu vain kerran palveluun. Käyttäjän tarvitsee

syöttää vain yksi käyttäjätunnus/salasana. Tämän jälkeen hänelle suodaan pääsy useaan eri sovellukseen. Prosessi todentaa käyttäjän kaikkiin sovelluksiin, joihin hänelle on annettu käyttöoikeus. (Rouse 2010, haettu 3.3.2016.)

Palvelun avulla voit yhdistää useita sovelluksia omassa verkossa, jotka käyttävät yhteistä todennusmekanismia. Nämä palvelut vaativat ja tarkistavat käyttäjätunnuksesi, kun kirjaudut verkkoon. Käyttäjätunnusten perusteella määritetään toiminnot, jotka voit suorittaa. Esimerkiksi, jos sovellukset ovat integroitu Kerberoksen kanssa, kun järjestelmä todentaa käyttäjätunnuksen, voit käyttää kaikkia resursseja, mitkä ovat integroitu Kerberoksen kanssa. (Microsoft 2016, haettu 3.3.2016.)



Kuva 5. Kertakirjautuminen.

8 MULTI-FACTOR AUTHENTICATION

8.1 Yleistä

MFA on yksinkertaisesti moninkertainen tunnistus. Sen tarkoituksena on todentaa käyttäjä useammalla kuin yhdellä vahvistustavalla. Se lisää toisen kriittisen kerroksen turvallisuutta käyttäjän todennuksiin. MFA toimii niin, että käyttäjältä vaaditaan kaksi tai useampi todentamismenetelmä:

- *jotain tietoa* (salasana)
- *jokin esine* (luotettava tavara, kuten puhelin)
- *jotain mitä olet* (biometrinen tunnistus)

(Mathers 2016, haettu 24.3.2016.)

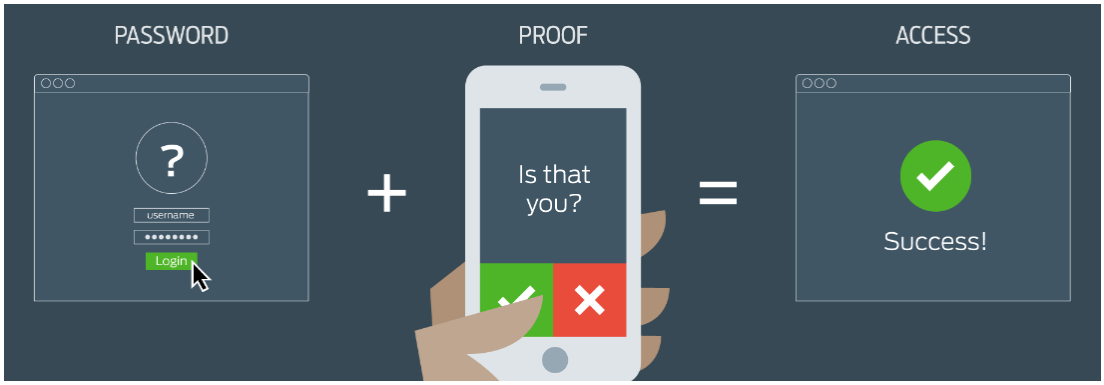
Multi-factor authentication viittaa yllämainittujen menetelmien käyttöön. Sen voima todentamismenetelmänä mitataan kyvyllä käyttää useita tunnistuksia. Kahta menetelmää käyttävä järjestelmä on vahvempi kuin yhtä menetelmää käyttävä. Kaikkia kolmea menetelmää käyttävä järjestelmä on huomattavasti vahvempi kuin kahta menetelmää käyttävä järjestelmä. (Burr, Dodson, Newton, Perlner, Polk, Gupta & Nabbus 2013, 20)

8.2 Uhat

Hyökkääjä voi saada haltuunsa todentamismenetelmän ja naamio sen näyttämään tunnuksen omistajalta. Uhat menetelmiä kohtaa voidaan lokeroida tavalla mihin hyökkäys kohdistuu:

- *jotain tietoa* on saattanut päätyä hyökkääjälle. Hyökkääjä voi arvata salasanan tai PIN-koodin. Se saatetaan lukea tallenteista tai päiväkirjasta. Järjestelmä saattaa sisältää haittaohjelman (näppäinnauhuri). Hyökkääjä voi myös opetella käyttäjän syntymäajan tai lemmikin nimen, ja tätä kautta yrittää arvata salasanan.
- *jokin esine* saattaa kadota, mennä rikki, varastetaan tai kloonataan käyttäjältä hyökkääjän toimesta. Esimerkiksi käyttäjän ohjelmistoon voidaan päästä käsiksi ja sitä kautta kopioidaan todentamismenetelmä. Laitteistoa voidaan manipuloida, varastaa tai duplikoida.
- *jotain mitä olet* voidaan replikoida. Hyökkääjä voi saada kopion käyttäjän sormenjäljestä ja pystyy siitä luomaan replikaatin.

(Burr ym. 2013, 47)



Kuva 6. Multi-Factor Authentication toiminta.

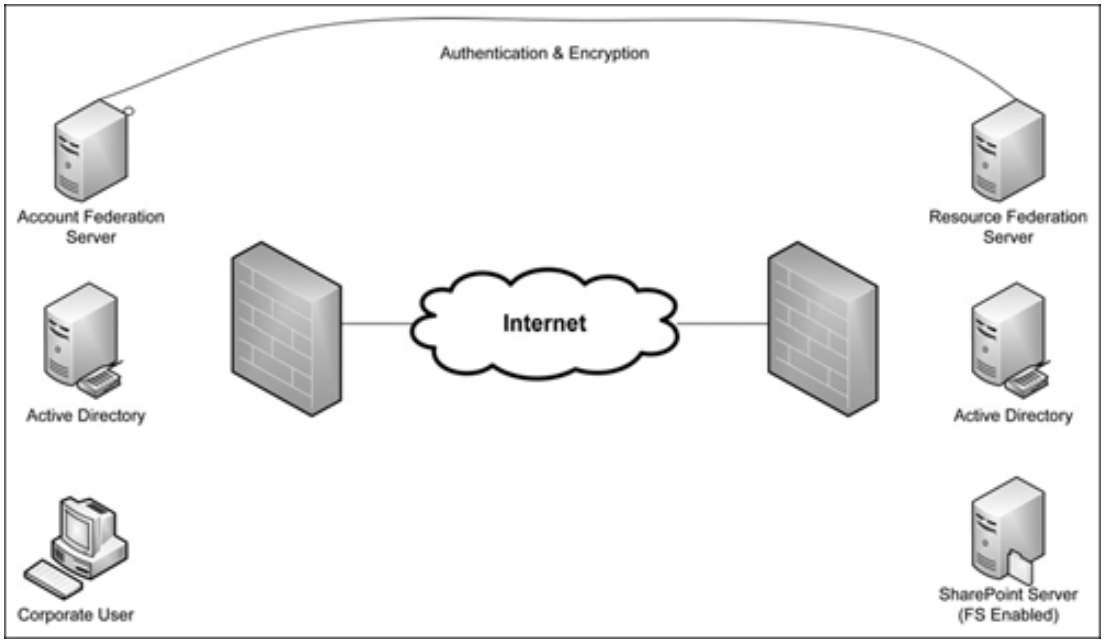
9 ACTIVE DIRECTORY FEDERATION SERVICES

9.1 Yleistä

ADFS on tarkoitettu olemaan yksinkertainen, turvallinen identiteettien federaatio ja verkon single sign-on ominaisuuksilla oleva rooli loppukäyttäjille, jotka haluavat käyttää sovelluksia ADFS:n sisällä, toisessa kumppaniorganisaatiossa tai pilvessä. (Microsoft 2014, haettu 3.3.2016.)

Windows Server 2012 R2 versiossa ADFS sisältää federaatio palveluroolin, joka toimii identiteettien tuottajana. Eli palvelu todentaa käyttäjän ja antaa hänelle pääsyn palveluihin, jotka luottavat ADFS:een. (Microsoft 2014, haettu 3.3.2016.)

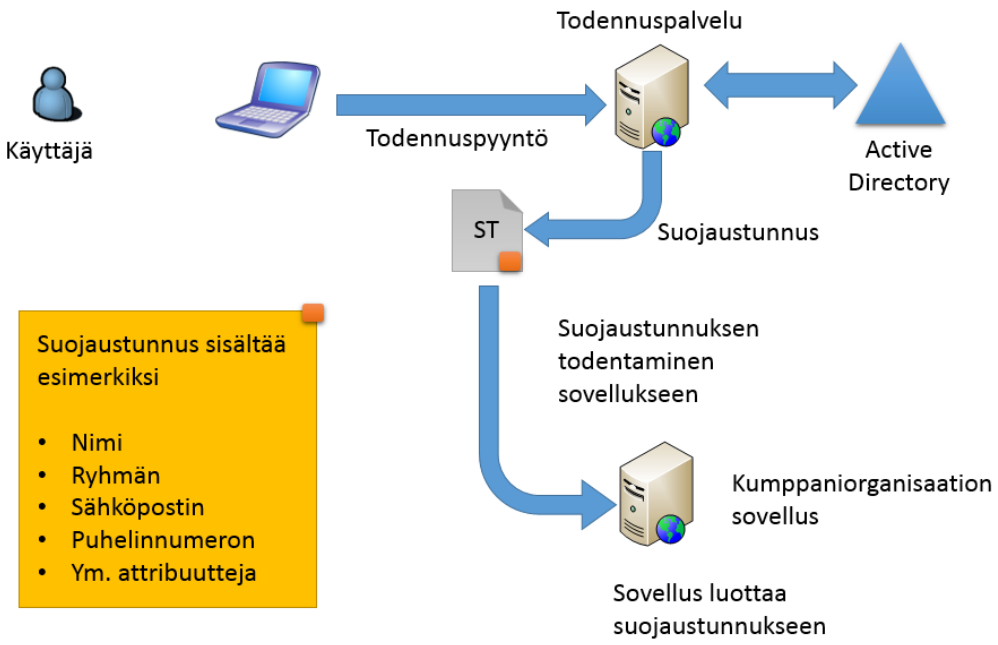
Microsoftin perinteinen Active Directory tallentaa käyttäjätunnukset sekä salasanat ja käyttää niitä hallitakseen sallittuja pääsyjä palveluihin toimialueen sisällä. Samalla se tarjoaa kertakirjautumisen yrityksen palveluihin. ADFS on rakennettu hyödyntämään tätä palvelua niin, että se kykenee todentamaan käyttäjät kolmannen osapuolen järjestelmiin, kuten toisen organisaation verkko tai sovellus, jota hallinnoidaan pilvestä. (Rouse 2013, haettu 3.3.2016.)



Kuva 7. ADFS toiminta.

9.2 Toimintaperiaate

Olemassa oleva käyttäjä haluaa käyttöön kumppaniorganisaation sovelluksen. Käyttäjä lähettää todennuspyynnön palveluun, joka hallinnoi identiteettejä ja jakaa suojaustunnuksia. Tässä kohtaa suojaustunnuksia jakava palvelu ottaa yhteyden Active Directoryyn. AD tunnistaa käyttäjän ja myöntää luvan jatkaa. Suojaustunnuksella käyttäjä todennetaan kumppaniorganisaation sovellukseen. Sovellus itse luottaa suojaustunnukseen ja täten ei itse joudu enää todentamaan käyttäjää erikseen. Sovellus tekee todennukset perustuen suojaustunnuksen sisältämiin tietoihin. (Craddock 2010, haettu 24.3.2016)

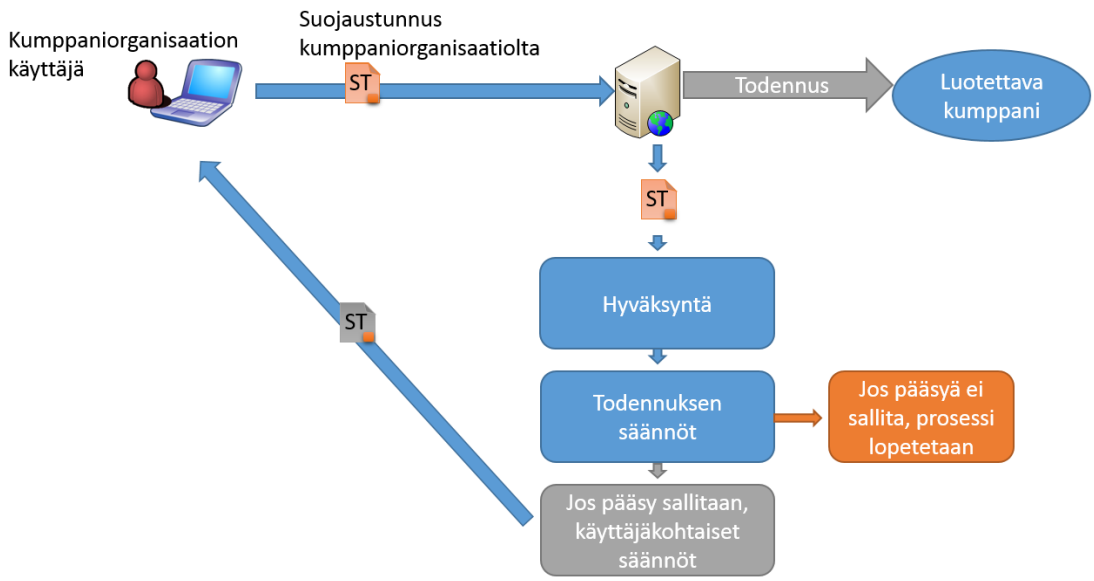


Kuva 8. Todennus ja suojaustunnus.

ADFS voi ainoastaan käyttää AD:ta identiteettien varastona todennusta varten. Todennus luo suojaustunnuksen, jossa ovat tiedot käyttäjästä ja käyttäjän ryhmästä. (Craddock 2010, haettu 24.3.2016)

9.3 Kumppaniorganisaatio

Identiteetille luodaan kehys, jota kaikki sovellukset voivat käyttää riippumatta heidän paikasta. Kumppaniorganisaatioille on annettava oikeus päästä sisään järjestelmiin, jossa todennetaan käyttäjät. Kumppaniorganisaatioiden välillä toimii luottamussuhde, eli oma suojaustunnuspalvelu luottaa kumppaniorganisaation suojaustunnuksiin, jotka sisältävät tiedot kumppaniorganisaation käyttäjistä. Oma suojaustunnuspalvelu ei ole vastuussa käyttäjien identifioimisesta, mutta silti prosessoi kirjautumiset. (Craddock 2010, haettu 24.3.2016)



Kuva 9. Kumppaniorganisaation käyttäjän todennus.

Käyttäjätiedot viedään läpi kolmen eri säännön kautta:

1. Sallitaanko käyttäjä kumppaniorganisaation sääntöjen mukaisesti (Hyväksyntä)
2. Todennetaan käyttäjän pyynnöt (Todennus)
3. Sallitaan käyttäjä ja hyväksytään pyyntö (Kuljetus)

(Beraud & Grasset, 97.)

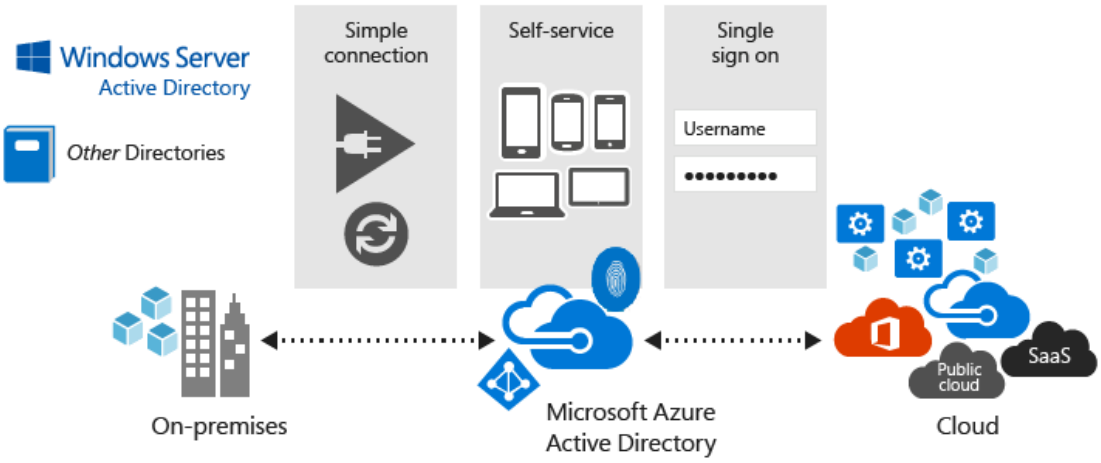
10 AZURE ACTIVE DIRECTORY

10.1 Yleistä

Azure Active Directory (Azure AD) on Microsoftin luoma pilvipalvelu, jonka tarkoituksena on hyödyntää käyttäjähakemistoa ja identiteetinhallintaa. Azure AD käyttää kertakirjautumista. Näin pystytään hyödyntämään sovelluksia kuten Office 365, Salesforce.com, Dropbox ja Concur. (Vilcinskas 2016, haettu 25.2.2016.)

Azure AD:n avulla voidaan identiteetinhallinnan lisäksi tehdä laitteiden rekisteröintejä, hallinnoida vahvoja tunnistautumisia, itsepalvelu salasanojen hallinnalle, ryhmien hallinta, etuoikeutetut käyttäjätilit, tiettyjen roolien pääsyoikeudet, sovellusten monitorointi, turvallisuuden seuranta ja hälytykset. (Vilcinskas 2016, haettu 25.2.2016.)

Azure AD voidaan integroida olemassa olevien Windows palvelimien käyttäjähakemistojen kanssa, jolloin organisaation paikalliset identiteetit pääsevät käyttämään pilvipalveluita. (Vilcinskas 2016, haettu 25.2.2016.)



Kuva 10. Azure AD:n toimintaperiaate.

10.2 Identiteettimallit

Azure AD vaatii käyttäjien olevan kirjautuneena sisään, jos he haluavat käyttää palveluita. Tämän vuoksi Azure on laatinut kaksi identiteettiä. Ensimmäinen on pilvi-identiteetti. Tämä identiteetti annetaan käyttäjälle, kun hän kirjautuu Azureen. Identiteetti on erillinen siitä minkä yritys on antanut paikallista kirjautumista varten. Näitä identiteettejä hallinnoidaan pilvessä Azure AD:ssa. (Beraud & Grasset, 15.)

Toinen identiteettimalli on federoitu identiteetti. Yritys jolla on paikallinen identiteettien hakemistopalvelu (Active Directory) voi laajentaa käyttäjätunnusten oikeuksia käyttämään single-sign on toimintoa. Tämän jälkeen käyttäjät voivat kirjautua

Azureen käyttäen samoja tunnuksia, joilla he kirjautuvat paikallisesti yrityksen tietokoneisiin. Tunnuksia hallinnoidaan paikallisesti ja synkronoidaan yrityksen Azure AD:n kanssa. Eli identiteetit pilvessä ovat synkronoituja kopioita paikallisista käyttäjätunnuksista. (Beraud & Grasset, 15.)

10.2.1 Pilvi-identiteetti

Ensimmäinen malli on yksinkertaisin. Tunnus luodaan Azure AD:ssa salasanan kanssa. Niin kuin nimi viittaa, identiteetti sijaitsee ainoastaan pilvessä. (Beraud & Grasset, 18.)

Käyttäjät kirjautuvat käyttäen heidän pilvi-identiteettiä. Pilvi-identiteetit todennetaan normaalilla kysyntä/vastaus tyylillä, jossa käyttäjät kirjoittavat käyttäjätunnuksen (esim. johndoe@yritys.fi) ja siihen liittyvän salasanan. Todennus tapahtuu pilvessä ja nämä käyttäjätiedot voidaan tarkistaa Azure AD:sta. Käyttäjät joutuvat aina kirjoittamaan käyttäjätiedot. (Beraud & Grasset, 18.)

Pilvi-identiteetillä ei ole suoraa vastaavuutta toisen käyttäjähakemiston kanssa. Tarkoittaen siis, että käyttäjillä on kaksi identiteettiä:

1. ensimmäinen jolla he kirjautuvat paikallisiin sovelluksiin ja resursseihin
2. toinen mitä käytetään Azure AD:n kirjautumisissa

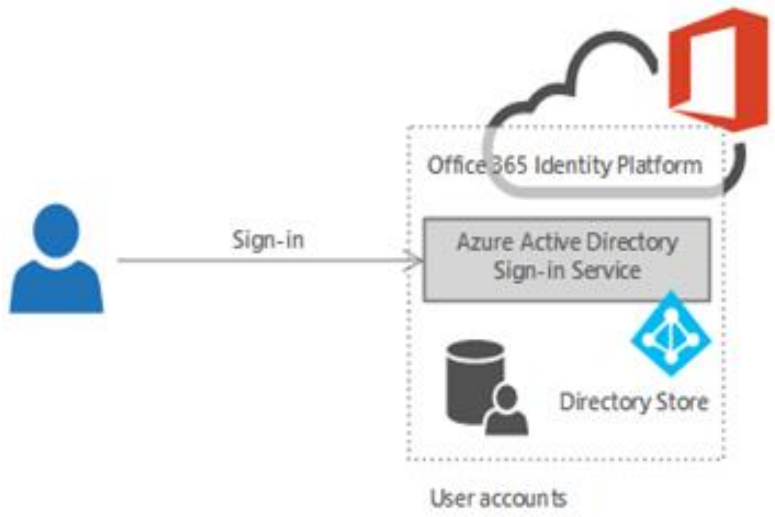
(Beraud & Grasset, 18.)

Jos käyttäjät kuuluvat yritykseen, joka käyttää Active Directorya paikallisesti, paikallinen käyttäjätunnus voi olla sama (johndoe@yritys.fi). Tässä pitää vain huomioida, että tunnukset pilven ja paikallisen palvelun kanssa ovat eri tunnuksia. Eli vaikka käyttäjät olisivat kirjautuneet paikalliseen AD:hen, he joutuvat kirjautumaan erikseen sisään Azure AD:hen. (Beraud & Grasset, 18.)

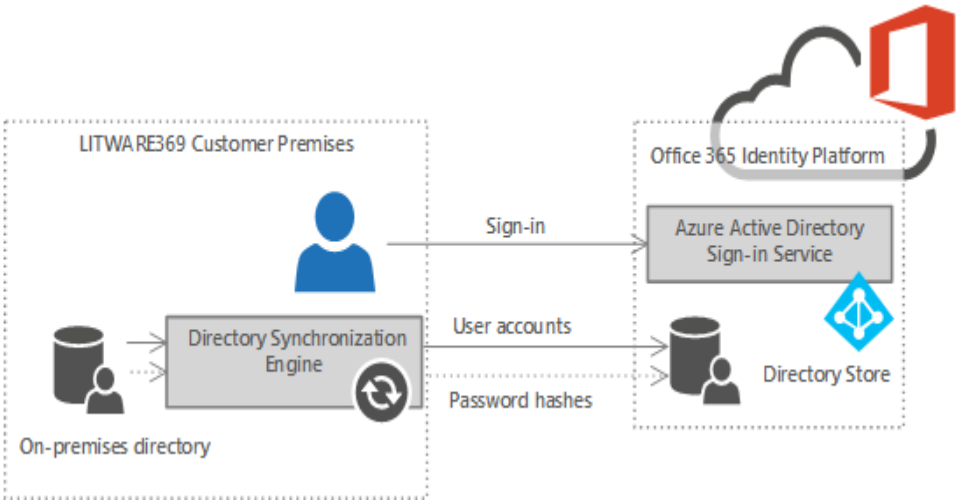
10.2.2 Federoitu identiteetti

Federoitu identiteetti eli synkronoitu identiteetti sallii paikallisen käyttäjähakemiston olevan synkronoituna Azuren käyttäjähakemiston kanssa. Eli se luo todellisen integraation paikallisesta käyttäjähakemistosta Azureen synkronoiden identiteetit ja ryhmät sekä mahdolliset salasanojen tiivisteet. (Beraud & Grasset, 20.)

Federoidun identiteetin hyötynä voidaan pitää sitä, että se sallii käyttäjien hallinnan suoraan Active Directorysta Users and Computers -ikkunan kautta. Tyypilliset järjestelmänvalvojan tehtävät koskien käyttäjätilejä, kontakteja, ryhmiä, tilien aktivointeja tehdään paikallisesta Active Directorysta ja ne replikoituvat Azure AD:n kanssa kolmen tunnin sisällä. (Beraud & Grasset, 21.)



Kuva 11. Pilvi-identiteetin malli.



Kuva 12. Synkronoitu identiteetti.

11 LOPUKSI

Tutkiskelun jälkeen voidaan todeta, että suuret ja myös pienemmät yritykset hyötyvät Active Directoryn käytöstä. Suuria käyttäjämääriä voidaan keskitetysti hallita yhdellä ohjelmalla. Hallinta tietysti vaatii AD:n tuntemusta. AD:n omat organisaatioyksiköt eivät välttämättä ole kaikista parhaimpia. Olisi suotavaa, että jokainen yritys tekisi omat organisaatioyksiköt. Tämä auttaisi hallinnassa ja selkeyttäisi henkilökuntaa. Organisaatioyksiköt voisivat olla: ylemmät toimihenkilöt, talous, opettajat, oppilaat. Ongelmatapauksissa käyttäjätilit olisi helpommin navigoitavissa omista organisaatioyksiköistä kun, että kaikki olisivat samassa isossa läjässä. Samalla tavalla tietokoneet ja resurssit voitaisiin lokeroida omiin yksiköihin: 1.kerros, 2.kerros, varalla.

Työn lopuksi voidaan vain todeta, että oma innostukseni vain kasvoi. Kirjallisuuden lukeminen ja omien kokemusten yhtenäistäminen toivat uutta uskoa AD:n käytöstä tulevaisuutta kohden. Active Directory tulee takuulla olemaan yksi asioista, jota IT-tradenomin tulee osata käyttää. Vaikka tämä kyseinen työ oli vain pintaraapaisu ja käsitteli käyttäjien hallintaa, on ainakin yksi siivu massiivisesta Active Directorysta tutkittu.

KIRJALLISET LÄHTEET

Beraud, P. & Grasset, J-Y. 2016 Azure AD/Office 365 Single Sign-On with AD FS in Windows Server 2012 R2 – Part 1 Haettu 13.4.2016. https://www.microsoft.com/en-us/download/details.aspx?id=36391

Bradley, T. 2011. Pros and Cons of Bringing Your Own Device to Work Haettu 12.4.2016. http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

Burr, W., Dodson, D., Newton, M., Perlner R., Polk, T., Gupta, S. & Nabbus, E. Electronic Authentication Guideline 2013. Haettu 21.4.2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Carter, J. 2012. Cloud computing explained Haettu 12.4.2016. http://www.techradar.com/news/internet/cloud-computing-explained-1105688

Craddock, J. 2010. Active Directory Federation Services How does it really work? Haettu 24.3.2016. http://download.microsoft.com/download/0/4/A/04ACF0B3-4B39-4DD1-86B5-FF0A6C110E9B/Active_Directory_Federation_Services.pptx

Desmond, B., Richards, J., Allen, R. & Lowe-Norris, A-G. 2013. Active Directory. Sebastopol, Kalifornia. O´Reilly Media, Inc.

Deuby S. 2013. Windows Server 2012 R2 Active Directory Embraces BYOD. Haettu 20.4.2016. http://windowsitpro.com/windows-server-2012-r2/windows-server-2012-r2-active-directory-embraces-byod

Hephaestus Books. Microsoft Office Servers, including: Active Directory, Domain Controller, Flexible Single Master Operation, Group Policy, Administrative Template, Directory Services Restore Mode, Paramount Defenses, File Replication Service, Ac-tive Directory Explorer.

Kivimäki, J. 2004. Inside Active Directory – verkonhallinta. Helsinki: Edita Prima OY. Haettu 3.3.2015. https://ekirjat.samk.fi/opiskelijat/itcd/InsideActiveDirectoryverkonhallinta.pdf

Kivimäki, J. 2005. Windows Server 2003 - Tehokas Hallinta. Jyväskylä. Gummeruksen Kirjapaino Oy.

Mathers, B. 2016. What is Azure Multi-Factor Authentication? Haettu 24.3.2016. https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/

Microsoft 2014. Active Directory Federation Services Overview Haettu 3.3.2016. https://technet.microsoft.com/library/hh831502

Microsoft 2014. What Are Domains And Forests? Haettu 15.4.2016. https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx

Microsoft 2014. Windows Authentication Concepts. Haettu 15.4.2016. https://technet.microsoft.com/en-us/library/dn751046.aspx

Microsoft 2016. Active Directory Objects. Haettu 21.4.2016. https://technet.microsoft.com/en-us/library/cc977990.aspx

Posey B. 2006 Networking Basics: Part 5 – Domain Controllers. Haettu 26.4.2016. http://www.windowsnetworking.com/articles-tutorials/netgeneral/Networking-Basics-Part5.html

Rouse, C. 2010. single sign-on (SSO) Haettu 3.3.2016. http://searchsecurity.techtarget.com/definition/single-sign-on

Rouse, M. 2013. Active Directory Federation Services (AD Federation Services) Haettu 3.3.2016. http://searchmobilecomputing.techtarget.com/definition/Active-Directory-Federation-Services-AD-Federation-Services

Shinder, T., Shinder D. & Martin J. 2003. MCSE Exam 70-294 Study Guide and DVD Training System: Planning, Implementing and Maintaining a Windows Server 2003 Active Directory Infrastructure. Missouri. Syngress Publishing. Haettu 3.3.2015. http://site.ebrary.com.lillukka.samk.fi/lib/SAMK/reader.action?docID=10044835

Stanek, W. 2003. Microsoft Windows Server 2003: asiantuntijan käsikirja. Helsinki: IT Press. Haettu 3.3.2015. https://ekirjat.samk.fi/opiskelijat/itcd/MicrosoftWindowsServer2003Asiantuntijankasikirja.pdf

Teleware Oy. Windows Aktiivihakemisto Esiluku. Haettu 25.2.2015. https://events.kpmg.fi/Portals/1/kurssit/windows%20active%20directory/EsilukuActiveDirectory.pdf

Tolvanen, P. 2011. Käsitteet ojennukseen: Active Directory (AD), LDAP, SSO ja identiteetinhallinta. Haettu 25.2.2015. http://intranet-ostajanopas.fi/2011/04/29/kasitteet-ojennukseen-active-directory-ad-ldap-sso-ja-identiteetinhallinta/

Vilcinskas, M. 2016. What is Azure Active Directory? Haettu 25.2.2016. https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

KUVALÄHTEET

Kuva 1. http://gitstack.com/wp-content/uploads/2012/04/new-user-gitstack-active-directory.png

Kuva 2. https://www.msi.umn.edu/sites/default/files/macRDP07.png

Kuva 3. https://ekirjat.samk.fi/opiskelijat/itcd/InsideActiveDirectoryverkonhal-linta.pdf

Kuva 4. https://ekirjat.samk.fi/opiskelijat/itcd/InsideActiveDirectoryverkonhal-linta.pdf

Kuva 5. http://blogs.vmware.com/vfabric/files/2013/03/authentication_chart.png

Kuva 6. http://www.it.northwestern.edu/images/ecommunicator/2015-winter/mul-tifactor.png

Kuva 7. http://programming4.us/image/102010/Active%20Directory%20Federa-tion%20Services_1.jpg

Kuva 8. http://download.microsoft.com/download/0/4/A/04ACF0B3-4B39-4DD1-86B5-FF0A6C110E9B/Active_Directory_Federation_Services.pptx.

Kuva 9. http://download.microsoft.com/download/0/4/A/04ACF0B3-4B39-4DD1-86B5-FF0A6C110E9B/Active_Directory_Federation_Services.pptx.

Kuva 10. https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

Kuva 11. https://www.microsoft.com/en-us/download/details.aspx?id=36391

Azure AD/Office 365 Single Sign-On with AD FS in Windows Server 2012 R2 – Part 1

Kuva 12. https://www.microsoft.com/en-us/download/details.aspx?id=36391

Azure AD/Office 365 Single Sign-On with AD FS in Windows Server 2012 R2 – Part 1